

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)11603 COLERAIN AVENUE, CINCINNATI, OHIO 45252  
[INCLUDING ALL OUTBUILDINGS AND CURTILAGE]Case No. **1:20-MJ-00053**

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the SOUTHERN District of OHIO, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| <i>Code Section</i> | <i>Offense Description</i>  |
|---------------------|---|
| 18 U.S.C. 2251      | Sexual Exploitation of Children   |
| 18 U.S.C. 2252      | Certain Activities Relating to Material Involving the Sexual Exploitation of Minors |
| 18 U.S.C. 2250      | Failure to Register   |

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

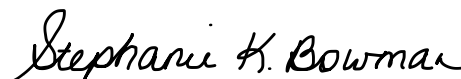


Applicant's signature

FBI/TFO MELISSA COOPER

Printed name and title

Sworn to before me and signed in my presence.

Date: Jan 23, 2020


Judge's signature

City and state: CINCINNATI, OHIO

HONORABLE STEPHANIE K BOWMAN, Magistrate Judge

Printed name and title

**ATTACHMENT A**

*Property to be searched*

The property to be searched is 11603 Colerain Avenue, Cincinnati, Ohio 45252, which is located along a private driveway along Colerain Avenue in Colerain Township of Hamilton, County, Ohio. The property is the first residence on the east side of the private drive. The property is a single residence two-story dwelling with red brick exterior and a green shingle roof. The door is wooden with decorative glass and has a white awning covering it.

There is a storage shed at the rear of the property.





**ATTACHMENT B**

*Property to be seized*

The terms "child pornography" and "visual depictions," as used herein, have the same definitions listed in "APPLICABLE STATUTES" section of the attached affidavit, and those definitions are incorporated herein by reference.

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, other memory storage devices and to include cellphones), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the production, possession, receipt, or distribution of child pornography, or to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography, visual depictions, or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, or visual depictions.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and

electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
13. Any and all cameras, film, videotapes or other photographic equipment.
14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation.
15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.
16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership



of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
18. Any images of Minor Victim A.
19. Any communications, in any format or medium, with Minor Victim A or other minors.
20. Any cameras to include any Motorola devices or information concerning the use, possession, or ownership of such Motorola devices.
21. Any records of interstate travel by Veerkamp or records of his place of residence.
22. To photograph or videotape the property.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION - CINCINNATI

IN THE MATTER OF THE SEARCH OF:  
11603 COLERAIN AVENUE, CINCINNATI,  
OHIO 45252

Case No. 1:20-MJ-00053

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Melissa Cooper, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 11603 Colerain Avenue, Cincinnati, Ohio 45252, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Colerain Township Police Department Detective currently assigned part-time to the violent crimes against children (VCAC) task force of the Federal Bureau of Investigation (FBI). I have been assigned to the FBI since May of 2013, investigating matters involving crimes against children, and other violent crimes. Also, during my tenure as a law enforcement officer which began in November of 2004, I have investigated a range of both state and federal criminal violations, including those involving national security investigations. I have received training in internet tools for criminal investigators, interviewing and interrogation techniques, arrest procedures, search and seizure, and various other crimes and investigation techniques.



3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

### **APPLICABLE STATUTES**

4. Title 18, United States Code § 2251(a), generally prohibits any person from using a minor to produce a visual depiction of a minor engaged in sexually explicit conduct, using materials that affect interstate commerce or if the visual depiction was transmitted or transported in interstate commerce. Sexually explicit conduct is defined in 18 U.S.C. § 2256(2)(A).

5. Title 18, United States Code § 2252, generally prohibits the transportation or shipping in interstate commerce the visual depictions of a minor engaging in sexually explicit conduct. It also prohibits the receipt, distribution, and possession of such visual depictions when involved in interstate or foreign commerce.

6. Title 18 United States Code § 2250, prohibits individuals who are required to register as sex offenders under the Sex Offender Registration and Notification Act who travel in interstate commerce and knowingly fail to register or update a registration as required by the act.

7. Title 18 United States Code § 2256 (2)(A) defines the term “sexually explicit conduct” as, i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; ii. Bestiality; iii. Masturbation; iv. Sadistic or masochistic abuse; or v. Lascivious exhibition of genitals or pubic area of any person.”

### **PROBABLE CAUSE**

8. On 11/24/2019, the Colerain Township Police Department received a walk in complaint at 4200 Springdale Road, Cincinnati, Ohio 45251. The complainant, Rachel McCullough, reported that she had found sexually explicit photos of a known female juvenile

(hereafter referred to as Minor Victim A) on her boyfriend Nicholas Veerkamp's laptop (hereafter referred to as the Device) in September of 2019. McCullough stated Minor Victim A depicted in the photos is in the fourth grade. McCullough also stated Minor Victim A is a neighbor of Veerkamp's friend who resides in West Harrison, Indiana and is believed to be that friend's step-father's niece.

9. After reporting the allegations, McCullough proceeded back to her residence and retrieved the Device and gave it to the Colerain Township Police Department. The Device was retrieved and placed into evidence under property tag # 42-14494.

10. On 12/4/2019 Colerain Township Detective Melissa Cooper made contact with McCullough who reported that the photos she observed on the laptop show Veerkamp's hand holding down the pants of the child and taking a photo of her vagina while she slept. Another photo was of the breast area of the child. The photos that were observed by McCullough were on Veerkamp's MacBook (the Device) and were in a file labeled "private". McCullough reported there were more photos and videos within the file some of which are innocent in nature but are of the same child. McCullough, Veerkamp, and Morghan Mahlke all lived together at the time she discovered the photos. Their residential address at the time of the incident was 8128 Hollybrook Court, Colerain Township, Ohio 45239. McCullough reported that they have lived there together since January of 2019.

11. McCullough stated she recently kicked Veerkamp out of the residence just prior to reporting the allegations. She reported that since she found the photos she had been upset but did not leave him at the time. She continued to live with Veerkamp until 11/24/2019 when she stated Veerkamp told her he was going to babysit his friend's kids at their home and that "set" her off. McCullough believes Veerkamp is residing back with his parents at 11603 Colerain Avenue, Cincinnati, Ohio 45252.

12. Colerain Township Police records show that on November 25, 2019, the Colerain Police were contacted to assist in the retrieval of property from 8128 Hollybrook Court, Colerain Township, Ohio 45239. Colerain Police Officer, Kevin Boyle, briefly met with the complainant, Morghan Mahlke in the vicinity of the residence prior to responding to 8128 Hollybrook Court. Mahlke explained that Veerkamp was on his way to the residence to retrieve his property and she didn't feel comfortable being there without police presence. Upon arrival to 8128 Hollybrook Court, the officer reported observing Veerkamp sitting in his vehicle parked in the driveway. Upon contact with Veerkamp, he stated he lived at the residence with McCullough and Mahlke and was there to get his belongings. Veerkamp stated he was having relationship problems and was moving out and back with his parents. Veerkamp retrieved his personal property from the address and left without incident. This incident was captured on the body camera of Officer Boyle.

13. On 12/6/2019, Detective Cooper spoke to Morghan Mahlke, the roommate of McCullough and Veerkamp. Mahlke stated she was at home the following day that Veerkamp stopped by the residence to pick up his belongings (11/25/2019). Mahlke stated Veerkamp "freaked" out when she told him his laptop was given to the Colerain Township Police Department. Mahlke stated he retrieved several items and left the residence. Mahlke stated that Veerkamp returned with his father the following day (11/26/2019), to pick up the remainder of his belongings. Mahlke stated that the three leased the home in January of 2019. A copy of the lease was provided by Rachel McCullough on 12/09/2019. The lease is for the residence at 8128 Hollybrook Court. All three of their names (McCullough, Mahlke, & Veerkamp) are on the lease. The lease states it began on January 1, 2019 and is for one year. Veerkamp's name is on the lease, but it appears as "Nicholas Jeerkamp" at the top of the lease but was signed at the bottom as "Nick Veerkamp".

14. In 2015, Veerkamp was charged with unlawful sexual conduct with a child. In 2016, Veerkamp pled to a lesser charge of Sexual Imposition. As a result of this conviction, Veerkamp was required to register as a sex offender. He registered with an address reflected as 11603 Colerain Avenue, Colerain Township, Ohio 45252. There is no known change of address on file reflecting Veerkamp ever registering at 8128 Hollybrook Court, Colerain Township, Ohio 45239 as a resident.

15. Pursuant to a search warrant issued by the US District Court for the Southern District of Ohio (Case No. 1:19MJ-856) investigators with the Hamilton County Sheriff's Office – Regional Electronic Crimes Investigations unit conducted a forensic exam of the Device. During the course of the examination a series of images were located at the following file paths: "Users/Nick/Documents/private/Photos(1)/" and "Users/Nick/Documents/private/Photos(1) 2/". The file folders include both explicit and non-explicit images of a prepubescent female who matched the likeness of the description of Minor Victim A provided by McCullough. The explicit image files included exif data<sup>1</sup> which indicated the images were created on October 21, 2017 between 11:42 and 11:45 UTC<sup>2</sup> with a Motorola brand device with a model of XT1254. The explicit images depicted Minor Victim A apparently asleep on a bed while a hand pulled down her pants and underwear to expose her genitals. Most of the images only depict the lower torso of Minor Victim A, to include her exposed genitals, and the hand of the other person. However, some images do depict Minor Victim A's genitals, her face, and the hand of the other person. An example of this is a file named: "IMG\_20171021\_034524109.jpg" located at the file path "Users/Nick/Documents/private/Photos(1)/". In addition to the apparent images of Minor Victim A, other images were located on the device which depicted what appeared to be currently

---

<sup>1</sup> EXIF data, also known as Exchangeable Image File Format, is metadata associated with an image file which can include a host of information such as creation date, location taken, device used, and other various camera settings.

<sup>2</sup> UTC is Universal Time Coordinated

unidentified prepubescent females nude and/or in sexually suggestive positions in which their genitals were exposed.

16. On January 22, 2020, investigators spoke with Ms. McCullough via telephone after sending her an e-mail with non-explicit images of the aforementioned series photos recovered from the Device. McCullough advised she did not recognize the “first girl” in the black t-shirt, however, the other photos are of Minor Victim A and the hand in the photo is that of Nicholas Veerkamp.

17. On 01/22/2020, investigators made contact with the Dearborn County Sheriff’s Department, School Resource Officer Jennifer Littiken. Investigators sent Officer Littiken an e-mail containing non-explicit images of Minor Victim A for identification purposes. Officer Littiken confirmed the identity of Minor Victim A, birthdate of XX-XX-2008 and has a residential address that is in the vicinity of the address provided by Ms. McCullough.

18. Law enforcement officers have observed Veerkamp’s vehicle parked at the PREMISES on several occasions in January 2020. Additionally, the vehicle Veerkamp used to retrieve his belongings from the Hollybrook residence has been observed at the PREMISES.

### **TECHNICAL TERMS**

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be

directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

20. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. *Probable Cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes



described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while

executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password

protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

23. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or

imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

25. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

### **CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

26. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

A. Those who receive and may be collecting child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

B. Those who receive and may be collecting child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

C. Those who receive and may be collecting child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist – that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years.

D. Likewise, those who receive and may be collecting child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

E. Those who receive and may be collecting child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

F. Those who receive and may be collecting child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

G. When images and videos of child pornography are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

27. Based upon the conduct of individuals involved in the collection of child pornography set forth in the above paragraph, namely, that they tend to maintain their collections at a secure, private location for long periods of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located at the SUBJECT PREMISES.

### **CONCLUSION**

28. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

### **REQUEST FOR SEALING**

29. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature



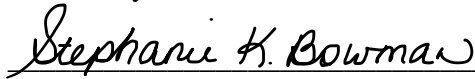
disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Detective Melissa Cooper  
FBI Task Force Officer

Subscribed and sworn to before me  
on January 22, 2020:



STEPHANIE K. BOWMAN  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF OHIO



**ATTACHMENT A**

*Property to be searched*

The property to be searched is 11603 Colerain Avenue, Cincinnati, Ohio 45252, which is located along a private driveway along Colerain Avenue in Colerain Township of Hamilton, County, Ohio. The property is the first residence on the east side of the private drive. The property is a single residence two-story dwelling with red brick exterior and a green shingle roof. The door is wooden with decorative glass and has a white awning covering it.

There is a storage shed at the rear of the property.





**ATTACHMENT B**

*Property to be seized*

The terms "child pornography" and "visual depictions," as used herein, have the same definitions listed in "APPLICABLE STATUTES" section of the attached affidavit, and those definitions are incorporated herein by reference.

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, other memory storage devices and to include cellphones), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the production, possession, receipt, or distribution of child pornography, or to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography, visual depictions, or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography, or visual depictions.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and

electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
13. Any and all cameras, film, videotapes or other photographic equipment.
14. Any and all visual depictions of minors in order to compare the images to known and identified minor victims of sexual exploitation.
15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.
16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership

of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
18. Any images of Minor Victim A.
19. Any communications, in any format or medium, with Minor Victim A or other minors.
20. Any cameras to include any Motorola devices or information concerning the use, possession, or ownership of such Motorola devices.
21. Any records of interstate travel by Veerkamp or records of his place of residence.
22. To photograph or videotape the property.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.